Appendix 5

HAWK - An Integrated Electronic Disease Surveillance System

Overview

HAWK is an integrated electronic disease surveillance system that was deployed in Kansas in September 1999. The basic characteristics of the system are:

- Thin-client, browser-based architecture for maximum flexibility and easy deployment and support;

- Internet-based: all transactions done through a secure TCP/IP connection;

- Accepts records for reportable diseases in Kansas;

- Can also accept records for diseases not reportable, but of public health importance in the state or in selected counties;

- All records are stored on a central server at the Kansas Department of Health and Environment;

- Multiple levels of security, including 128 bit SSL certificates, are built into the system;

- Multiple levels of confidentiality assure that specific records can be accessed only by selected authorized users;

- Report-generating capabilities for pre-defined reports (including tabulations and time analyses) and for custom-designed 2x3 reports;

System Description

At the core of the new system is an SQL database, which resides on a server within Kansas Department of Health and Environment (KDHE)'s firewall. The Internet server resides outside of the KDHE firewall and employs Internet Information Server 5.0 (IIS). Active Server Pages (ASP) runs on the IIS server and control database access from the IIS server to the SQL Server database. This client-server architecture permits rapid page access while protecting the actual data from unauthorized access.

The application logic is deployed to a three "tier" comprised of Microsoft IIS, ASPs, and Java on a public semi-secure DMZ network segment of KDHE's firewall. The back-end database (SQL Server 2000) is ODBC and SQL compliant and resides on the private, secure side of the firewall.

Individual 'pages' on the system were developed utilizing Microsoft Visual Studio 6.0. These pages incorporate many different technologies: java script, active server pages, and DHTML. All code utilized in the system is non-browser specific.

The disease reporting system offers a central, statewide database of reportable diseases that can be accessed remotely by authorized users via the Internet. For remote users such as local health departments the only system requirement is an Internet connection and a browser software (Netscape ver. 4.6 or higher or Internet Explorer version 6 or higher). Remote users will not only be able to report disease occurrence more efficiently, they will also be able to generate summary statistics to assist them in evaluating the overall effectiveness of public health efforts in their areas, and to identify at-risk populations. The system under development will also allow for state epidemiologists and laboratorians to update/correct patient records as needed.

HAWK was designed based on extensive inputs from users of the current NETSS-based electronic surveillance system. The system is patient-based: that means that each individual needs to be entered only once and can be linked to multiple events (i.e., disease reports). To report a case, users enter the patient name, which initiates a Soundex search for matching patient records currently in the database. Matching records are displayed and permit the user to select an already existing patient record and add a case record to it, or create a new patient record if needed. The patient information screen accepts basic patient information such as name, address, date of birth, and other demographic information. Individual patients may have more than one case record if they are diagnosed with more than one reportable disease (i.e., John Doe may have one record for salmonella with another record for Campylobacter). The case record screen accepts information on the disease being reported, date of onset, date of

diagnosis, date of laboratory confirmation, MMWR week, and whether the disease is outbreak associated. CDC standards (CIPHER) are followed for variable definitions throughout the database.

After the initial case report screen is submitted, subsequent pages are accessible based on what disease is being reported (e.g., laboratory results, x-ray, comments, etc.). There is a one-to-many relationship between the basic case record and some of the additional screens (such as the laboratory results screen), which permits multiple entries for each case record.

Selected diseases have extended epidemiological screens based on CDC reportable disease forms. Where information requested on these forms has already been entered, this information is automatically transferred to the appropriate field in order to make the reporting process less burdensome and to avoid potential data conflicts, which may be caused by user errors.

The system has expanded capacity for user-entered comments. From any screen in a patient record the user has the capacity to create a comment that is unlimited with respect to how much text can be entered. The number of comments per record is also unlimited, with previously entered comments accessible from a screen that lists each comment entry by topic and date created.

Summary statistics are available to all users. Reports may be generated for specific disease events on a statewide, regional, or local level. This empowers local users to better monitor disease events and trends in their locality.

Data Exchange

All disease reports (available in Epi-Info format since 1989) are being transferred into HAWK. The option to accept HL7 transactions from the KCMO laboratory is fully functional.

The system has the option to export basic case records into a spreadsheet and download the file to a local workstation for local offline processing. However, no transactions are possible in offline mode. Any of the reports generated can also be downloaded as a spreadsheet. The system also generates a NETSS-compatible ASCII file for transmission to CDC.

The first version of HAWK includes records for TB, for vaccine-preventable diseases, and for reportable diseases other than STD's and HIV/ AIDS. It is anticipated that in the first part of 2000 the system will also include STD's records. The option to add HIV/AIDS records will be explored later.

Security

KDHE recognizes the requirement for secure, high performance, reliable, inexpensive communications to "partners" such as county health departments, hospitals, laboratories, coroner's offices, etc. In 1997, KDHE implemented an Internet firewall to separate KDHE's private Intranet network resources from the public Internet.

Utilization of a public system such as the Internet to transmit confidential patient information with regards to reportable diseases raises security concerns. The system must be able to protect against unauthorized interceptions of usable patient information as it is transferred over the public Internet. Access to the database must be protected to prevent unauthorized users from entering the surveillance database, and once in the system, authorized users need to be limited to viewing confidential data for patients from their jurisdiction only. HAWK utilizes three security layers to protect confidential patient information from being accessed by unauthorized persons.

The first layer of security employs Secure Sockets Layer (SSL) technology. SSL encrypts all data communications between the clients and the server. This prevents the interception of confidential patient information as it is passed over the Internet. The SSL technology is imbedded within SQL Server 2000 and the browser and requires third party certification.

The second layer of security relies on user identification and passwords to prevent unauthorized users from accessing the disease reporting system. User ID's and passwords are sent to an Active Server Page (ASP) for processing. The ASP connects to the database and verifies the user ID and password. Once authenticated, a session is started between the web server ant the client. Without the creation of a session between the client and the server, no direct database access can occur.

The third layer of security prevents authorized users from accessing information, which they are not entitled to view. For example, a user from County Health Department A would not have authority to view confidential patient information for residents of County B. (The option to share information across jurisdictions is available in the system, if desired.) Also, only certain users within local health department A may have the rights to view information with respect to a patient's HIV status.

While HAWK will run under a Virtual Private Network (VPN) when one is available (e.g., between a local health department and the state office), its architecture (including the use of SSL and certificates of security technology) allows to achieve a high level of security also outside of a VPN environment. This makes the system available for authorized users such as hospitals and physician offices for whom a VPN connection is not a viable option.

H:\EPI\HAWK\ HAWK DESCRIPTION\HAWK description.rtf
May 2, 2002